# Topic: Reconnaissance using Nmap and Nessus

## 1.a Map the Network using nmap

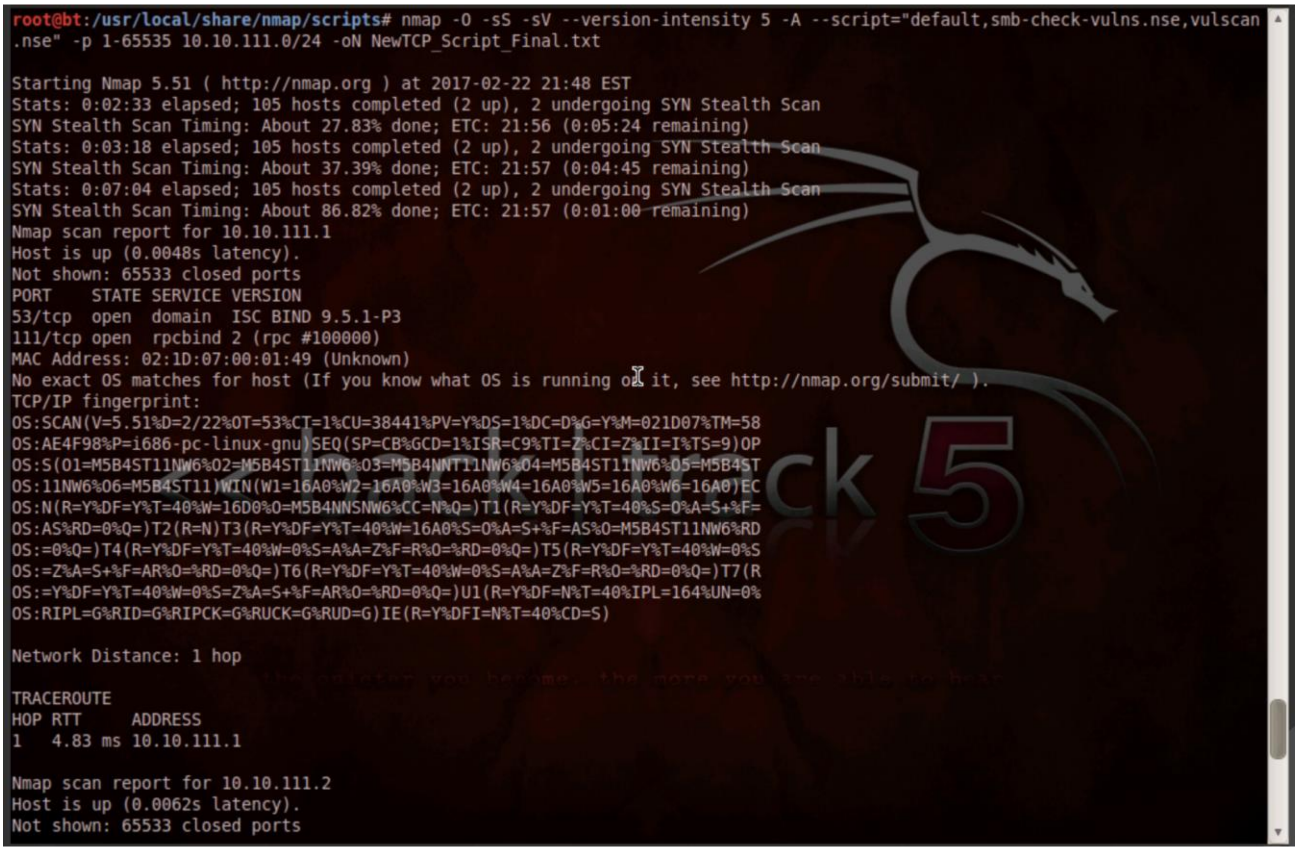
### Scan for all TCP Ports – OS Detection – Service Version and Vulnerability Scan

*Command:*

***nmap -O -sS -sV --version-intensity 5 -A –script="default,smb-check-vulns.nse,vulscan.nse"-p 1-65535 10.10.111.0/24 -oN NewTCP_Script_Final.txt***

- ⇨ *TCP SYN Scan -sS*
- ⇨ *Operating System Detect -O*
- ⇨ *Version Detect (sV) and Version Intensity (version-intensity)*
- ⇨ *OS Detect and Version (A)*
- ⇨ *Ports all – P(1-65535)*
- ⇨ *Vulnerability Script Execution*
  - *Default*
  - *Vuln, smb-check - Vulnerability Script – Known Vulnerability*
  - *VulScan - Updated the DB Initially calling -nmap -script-updatedb*
  - *Used Database – Exploit.db and allitems.db –Obtained from* [https://svn.nmap.org/nmap-exp/jiayi/scripts/vulscan.nse](https://svn.nmap.org/nmap-exp/jiayi/scripts/vulscan.nse)

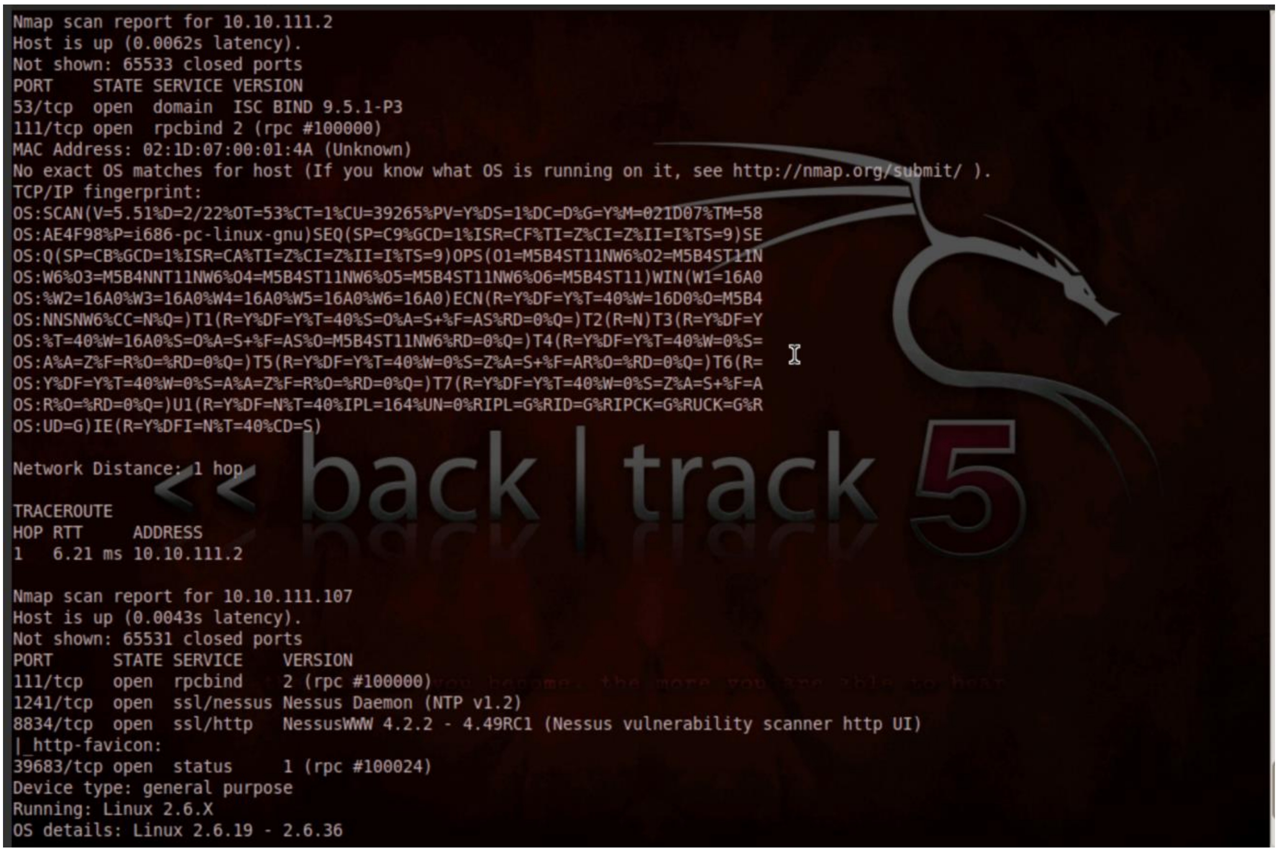
***Screens:***



```
root@bt:/usr/local/share/nmap/scripts# nmap -O -sS -sV --version-intensity 5 -A --script="default,smb-check-vulns.nse,vulscan
.nse" -p 1-65535 10.10.111.0/24 -oN NewTCP_Script_Final.txt

Starting Nmap 5.51 ( http://nmap.org ) at 2017-02-22 21:48 EST
Stats: 0:02:33 elapsed; 105 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.83% done; ETC: 21:56 (0:05:24 remaining)
Stats: 0:03:18 elapsed; 105 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.39% done; ETC: 21:57 (0:04:45 remaining)
Stats: 0:07:04 elapsed; 105 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.82% done; ETC: 21:57 (0:01:00 remaining)
Nmap scan report for 10.10.111.1
Host is up (0.0048s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE VERSION
53/tcp  open  domain  ISC BIND 9.5.1-P3
111/tcp open  rpcbind 2 (rpc #100000)
MAC Address: 02:1D:07:00:01:49 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=2/22%OT=53%CT=1%CU=38441%PV=Y%DS=1%DC=D%G=Y%M=021D07%TM=58
OS:AE4F98%P=i686-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=C9%TI=Z%CI=Z%II=I%TS=9)OP
OS:S(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST
OS:11NW6%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)EC
OS:N(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW6%RD
OS:=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   4.83 ms 10.10.111.1

Nmap scan report for 10.10.111.2
Host is up (0.0062s latency).
Not shown: 65533 closed ports
```

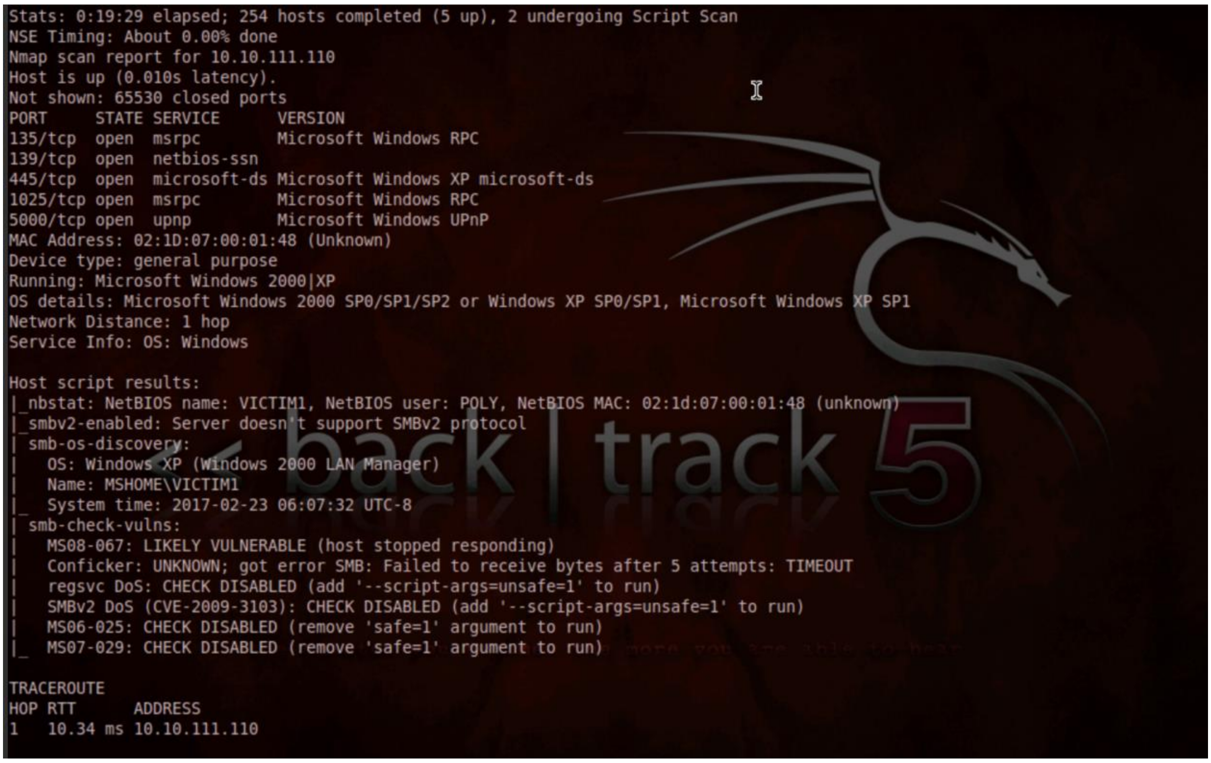
- ■ *Nmap starts the SYN scan by sending TCP SYN packets and waits for a SYNACK packet to discover if the port if open (A -tcp-connect option will establish full connection while the -syn option maintains a half way connection)*

- *Nmap detects the Operating System Running on the machine as well as the Services and Version running on the ports*



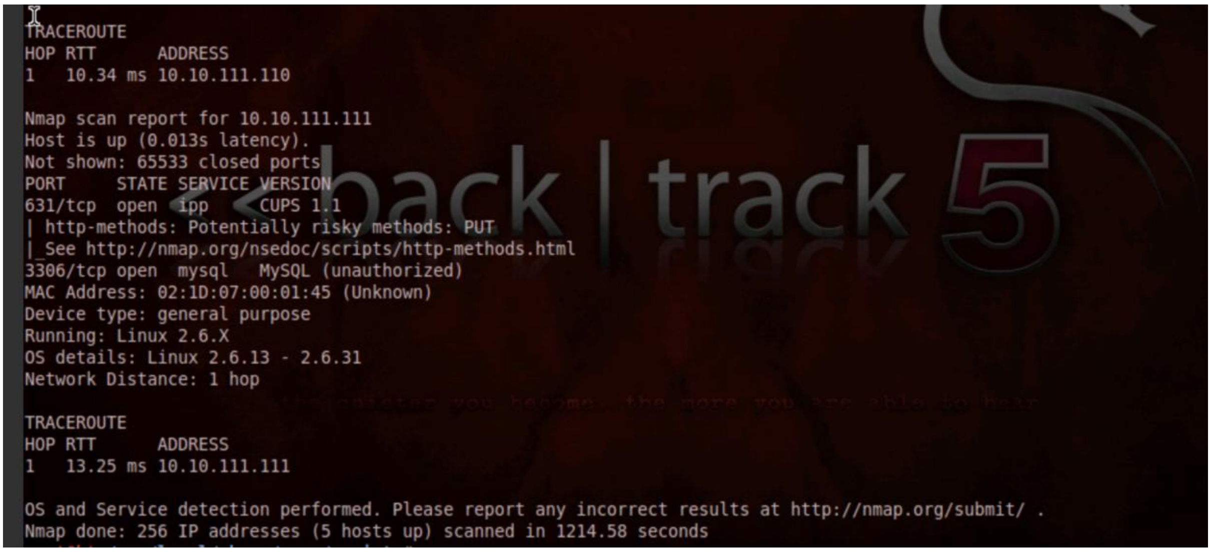
```
Nmap scan report for 10.10.111.2
Host is up (0.0062s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE VERSION
53/tcp  open  domain  ISC BIND 9.5.1-P3
111/tcp open  rpcbind 2 (rpc #100000)
MAC Address: 02:1D:07:00:01:4A (Unknown)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=2/22%OT=53%CT=1%CU=39265%PV=Y%DS=1%DC=D%G=Y%M=021D07%TM=58
OS:AE4F98%P=i686-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%TS=9)SE
OS:Q(SP=CB%GCD=1%ISR=CA%TI=Z%CI=Z%II=I%TS=9)OPS(O1=M5B4ST11NW6%O2=M5B4ST11N
OS:W6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST11)WIN(W1=16A0
OS:%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4
OS:NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y
OS:%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW6%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   6.21 ms 10.10.111.2

Nmap scan report for 10.10.111.107
Host is up (0.0043s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE    VERSION
111/tcp   open  rpcbind    2 (rpc #100000)
1241/tcp  open  ssl/nessus Nessus Daemon (NTP v1.2)
8834/tcp  open  ssl/http   NessusWWW 4.2.2 - 4.49RC1 (Nessus vulnerability scanner http UI)
|_http-favicon:
39683/tcp open  status     1 (rpc #100024)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.36
```

- *The Next Screen of host Windows shows potential vulnerability from the script run*



```
Stats: 0:19:29 elapsed; 254 hosts completed (5 up), 2 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.10.111.110
Host is up (0.010s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5000/tcp open  upnp         Microsoft Windows UPnP
MAC Address: 02:1D:07:00:01:48 (Unknown)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS details: Microsoft Windows 2000 SP0/SP1/SP2 or Windows XP SP0/SP1, Microsoft Windows XP SP1
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_nbstat: NetBIOS name: VICTIM1, NetBIOS user: POLY, NetBIOS MAC: 02:1d:07:00:01:48 (unknown)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   Name: MSHOME\VICTIM1
|_  System time: 2017-02-23 06:07:32 UTC-8
| smb-check-vulns:
|   MS08-067: LIKELY VULNERABLE (host stopped responding)
|   Conficker: UNKNOWN; got error SMB: Failed to receive bytes after 5 attempts: TIMEOUT
|   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_  MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

TRACEROUTE
HOP RTT      ADDRESS
1   10.34 ms 10.10.111.110
```

- *The Vulnerability Scripts execute and output the potential vulnerability scenario in the host. (SMB Server and Unauthorized MySQL Server)*



```
TRACEROUTE
HOP RTT      ADDRESS
1   10.34 ms 10.10.111.110

Nmap scan report for 10.10.111.111
Host is up (0.013s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
631/tcp  open  ipp     CUPS 1.1
| http-methods: Potentially risky methods: PUT
|_See http://nmap.org/nsedoc/scripts/http-methods.html
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 02:1D:07:00:01:45 (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.31
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   13.25 ms 10.10.111.111

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 1214.58 seconds
```

- *Nmap Scans the networks, Finds hosts in the network, performs TCP SYN scan and from the response obtained guesses from its database the Operating System, the version and service running in the host*

- *The TCP Scan Detects all the hosts present, their TCP Ports open and the corresponding OS, Service and Version running with the Potential Vulnerability data*

## 1.b Scan for top 30 UDP Ports:

Command:

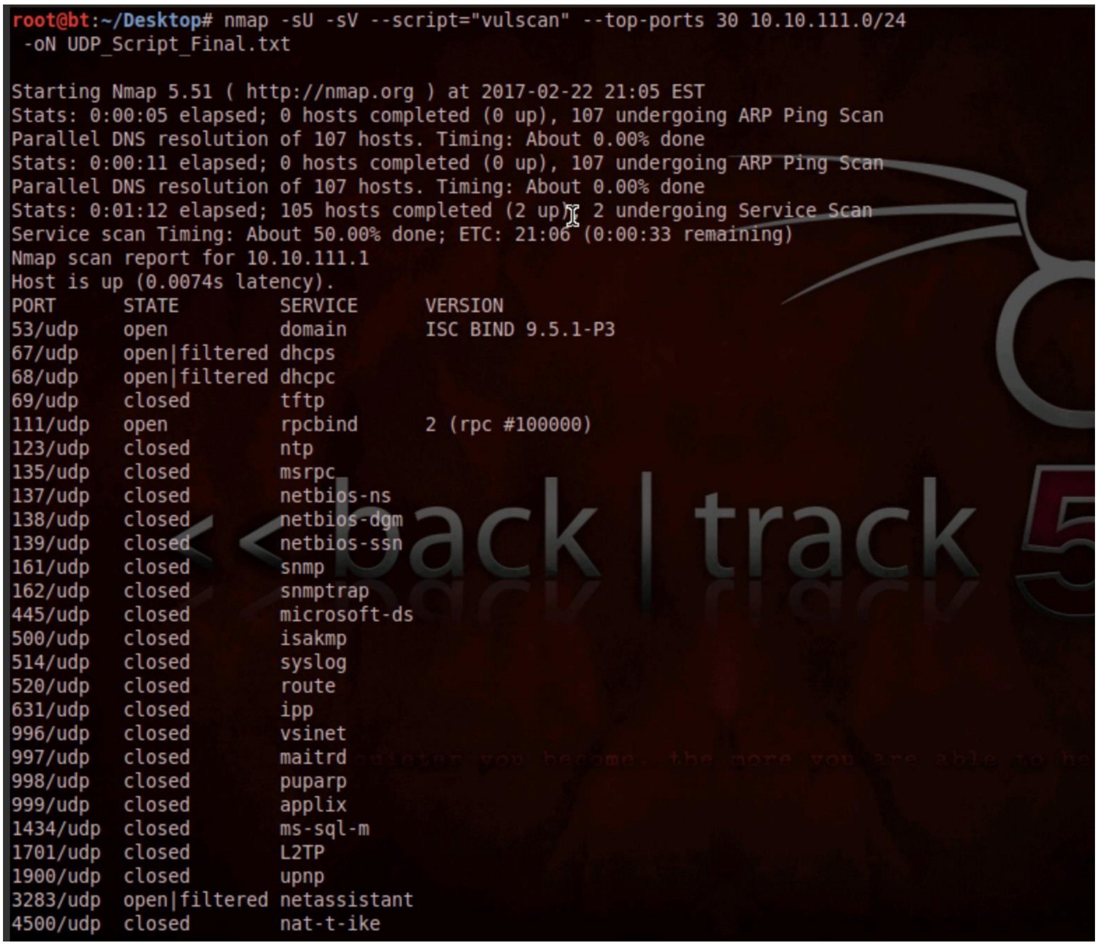
The command to perform the scan on the top 30 ports for UDP:

**nmap -sU -sV --script=”vulscan.nse” --top-ports 30 -oN UDP_Script_Final.txt 10.10.111.0/24**

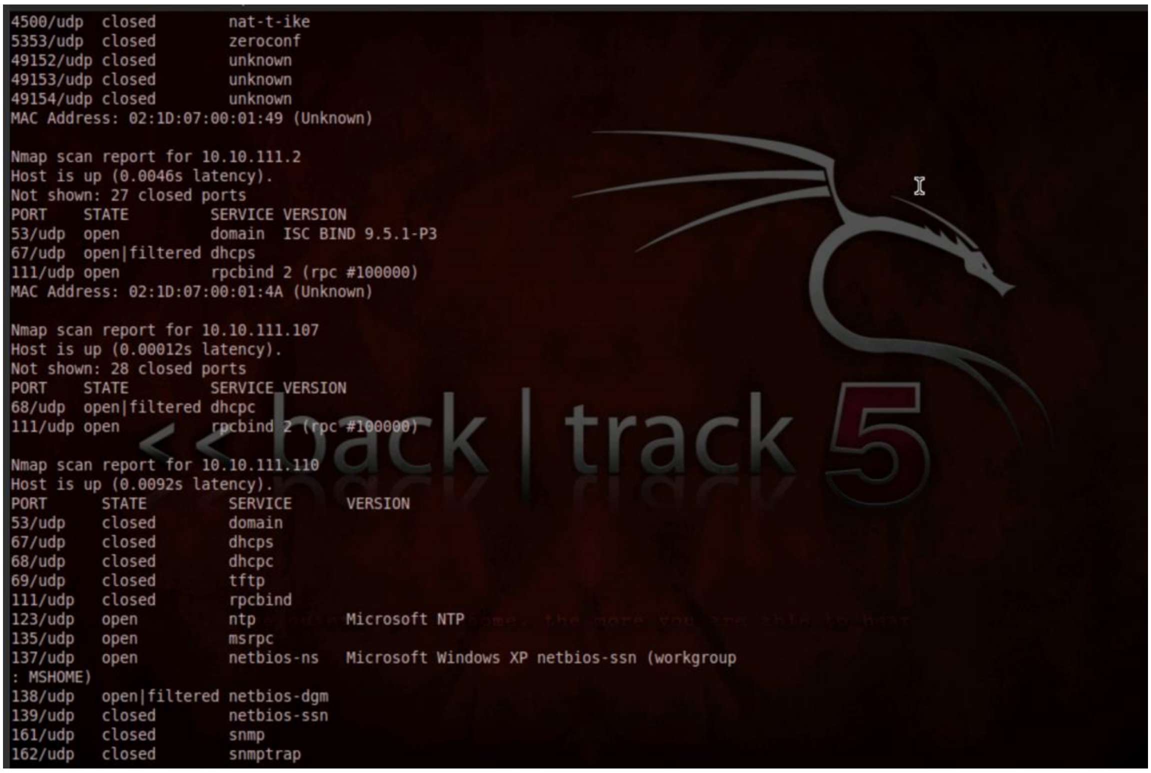
- ⇨ *UDP Scan (sU) for Top Ports – 30 (top-ports)*
- ⇨ *Service Detection (sV)*
- ⇨ *Script Run – VulScan – Vulnerability Script*

***Output:*** Nmap performs UDP Scans for the 30 top UDP Ports on all the hosts, lists their IP address and UDP Ports Open

- Additionally, Nmap also populates the Service and the Version running in those ports discovered

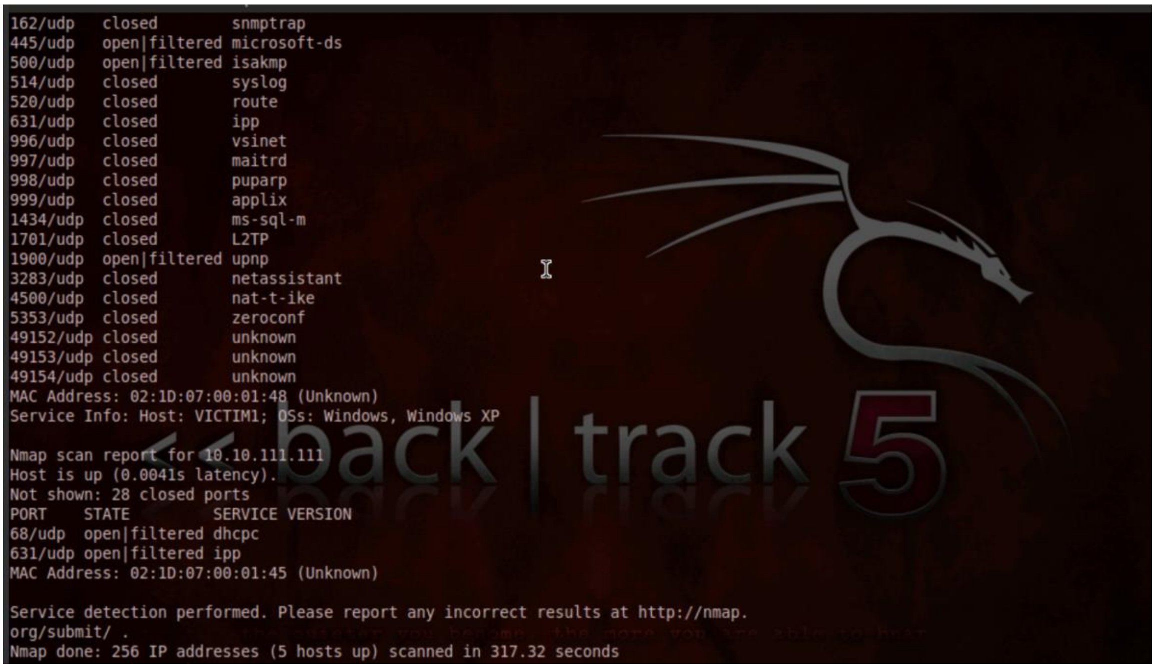


```
root@bt:~/Desktop# nmap -sU -sV --script="vulscan" --top-ports 30 10.10.111.0/24
 -oN UDP_Script_Final.txt

Starting Nmap 5.51 ( http://nmap.org ) at 2017-02-22 21:05 EST
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 107 undergoing ARP Ping Scan
Parallel DNS resolution of 107 hosts. Timing: About 0.00% done
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 107 undergoing ARP Ping Scan
Parallel DNS resolution of 107 hosts. Timing: About 0.00% done
Stats: 0:01:12 elapsed; 105 hosts completed (2 up), 2 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 21:06 (0:00:33 remaining)
Nmap scan report for 10.10.111.1
Host is up (0.0074s latency).
PORT      STATE         SERVICE      VERSION
53/udp    open          domain       ISC BIND 9.5.1-P3
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
111/udp   open          rpcbind      2 (rpc #100000)
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
996/udp   closed        vsinet
997/udp   closed        maitrd
998/udp   closed        puparp
999/udp   closed        applix
1434/udp  closed        ms-sql-m
1701/udp  closed        L2TP
1900/udp  closed        upnp
3283/udp  open|filtered netassistant
4500/udp  closed        nat-t-ike
```

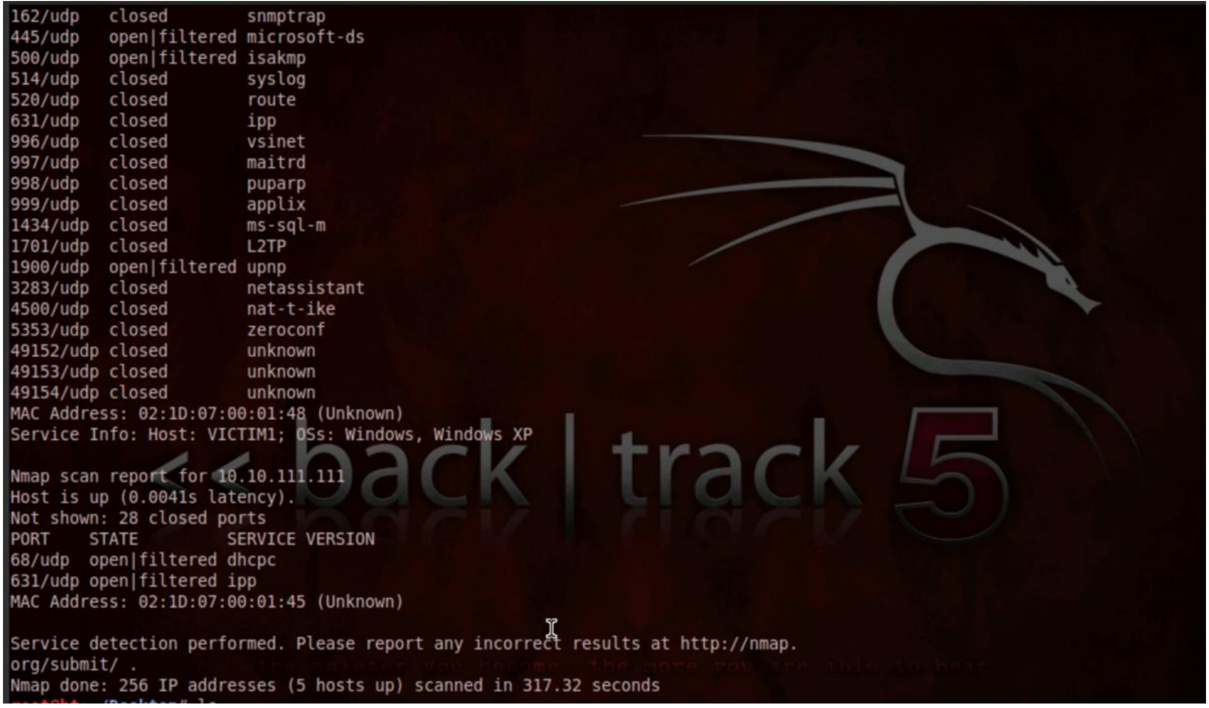


```
4500/udp  closed        nat-t-ike
5353/udp  closed        zeroconf
49152/udp closed        unknown
49153/udp closed        unknown
49154/udp closed        unknown
MAC Address: 02:1D:07:00:01:49 (Unknown)

Nmap scan report for 10.10.111.2
Host is up (0.0046s latency).
Not shown: 27 closed ports
PORT    STATE         SERVICE VERSION
53/udp  open          domain  ISC BIND 9.5.1-P3
67/udp  open|filtered dhcps
111/udp open          rpcbind 2 (rpc #100000)
MAC Address: 02:1D:07:00:01:4A (Unknown)

Nmap scan report for 10.10.111.107
Host is up (0.00012s latency).
Not shown: 28 closed ports
PORT    STATE         SERVICE VERSION
68/udp  open|filtered dhcpc
111/udp open          rpcbind 2 (rpc #100000)

Nmap scan report for 10.10.111.110
Host is up (0.0092s latency).
PORT      STATE         SERVICE      VERSION
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    closed        dhcpc
69/udp    closed        tftp
111/udp   closed        rpcbind
123/udp   open          ntp          Microsoft NTP
135/udp   open          msrpc
137/udp   open          netbios-ns   Microsoft Windows XP netbios-ssn (workgroup
: MSHOME)
138/udp   open|filtered netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
```

- *Nmap checks the well-known UDP ports for service detection for each host and provides the output. Hence the service type is already known and only the detection of OPEN/CLOSE matters*



```
162/udp   closed        snmptrap
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
996/udp   closed        vsinet
997/udp   closed        maitrd
998/udp   closed        puparp
999/udp   closed        applix
1434/udp  closed        ms-sql-m
1701/udp  closed        L2TP
1900/udp  open|filtered upnp
3283/udp  closed        netassistant
4500/udp  closed        nat-t-ike
5353/udp  closed        zeroconf
49152/udp closed        unknown
49153/udp closed        unknown
49154/udp closed        unknown
MAC Address: 02:1D:07:00:01:48 (Unknown)
Service Info: Host: VICTIM1; OSs: Windows, Windows XP

Nmap scan report for 10.10.111.111
Host is up (0.0041s latency).
Not shown: 28 closed ports
PORT    STATE         SERVICE VERSION
68/udp  open|filtered dhcpc
631/udp open|filtered ipp
MAC Address: 02:1D:07:00:01:45 (Unknown)

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 317.32 seconds
```



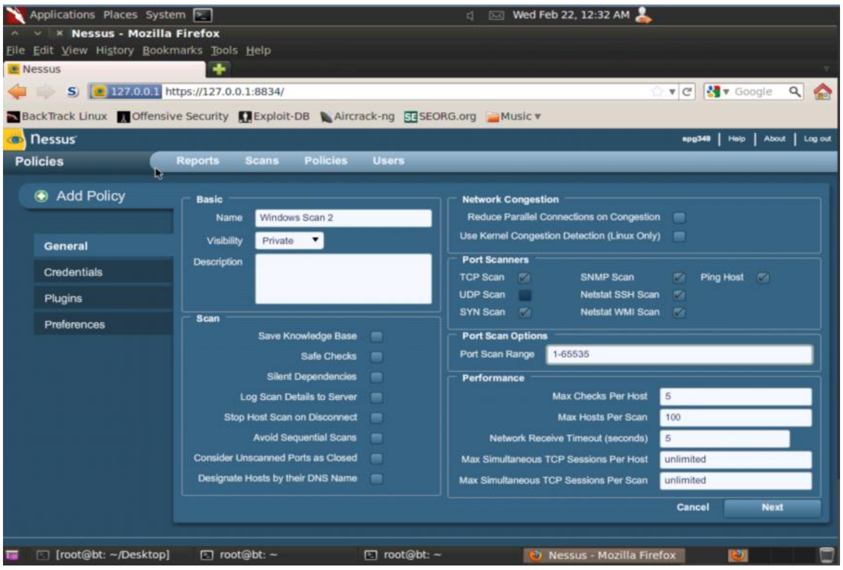
```
162/udp   closed        snmptrap
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
996/udp   closed        vsinet
997/udp   closed        maitrd
998/udp   closed        puparp
999/udp   closed        applix
1434/udp  closed        ms-sql-m
1701/udp  closed        L2TP
1900/udp  open|filtered upnp
3283/udp  closed        netassistant
4500/udp  closed        nat-t-ike
5353/udp  closed        zeroconf
49152/udp closed        unknown
49153/udp closed        unknown
49154/udp closed        unknown
MAC Address: 02:1D:07:00:01:48 (Unknown)
Service Info: Host: VICTIM1; OSs: Windows, Windows XP

Nmap scan report for 10.10.111.111
Host is up (0.0041s latency).
Not shown: 28 closed ports
PORT    STATE         SERVICE VERSION
68/udp  open|filtered dhcpc
631/udp open|filtered ipp
MAC Address: 02:1D:07:00:01:45 (Unknown)

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 317.32 seconds
```

- Nmap tries to send corresponding packets to the well-known UDP ports to gain a better response. UDP Scan takes more time to detect

## 1. Nessus Vulnerability Scan

## Nessus Setup:

- Create a User, Start the Nessus Server and Launch Client in Browser
- Login and Create a Policy
    - Enabled All possible scans (TCP, SYN, SNMP)
    - Removed Safe Checks to probe the system for any kernel failures
    - Port number selected for the entire range [1 - 65535]
    - The number of connections and other options are default



Add Policy — General

Basic
Name: Windows Scan 2
Visibility: Private
Description:

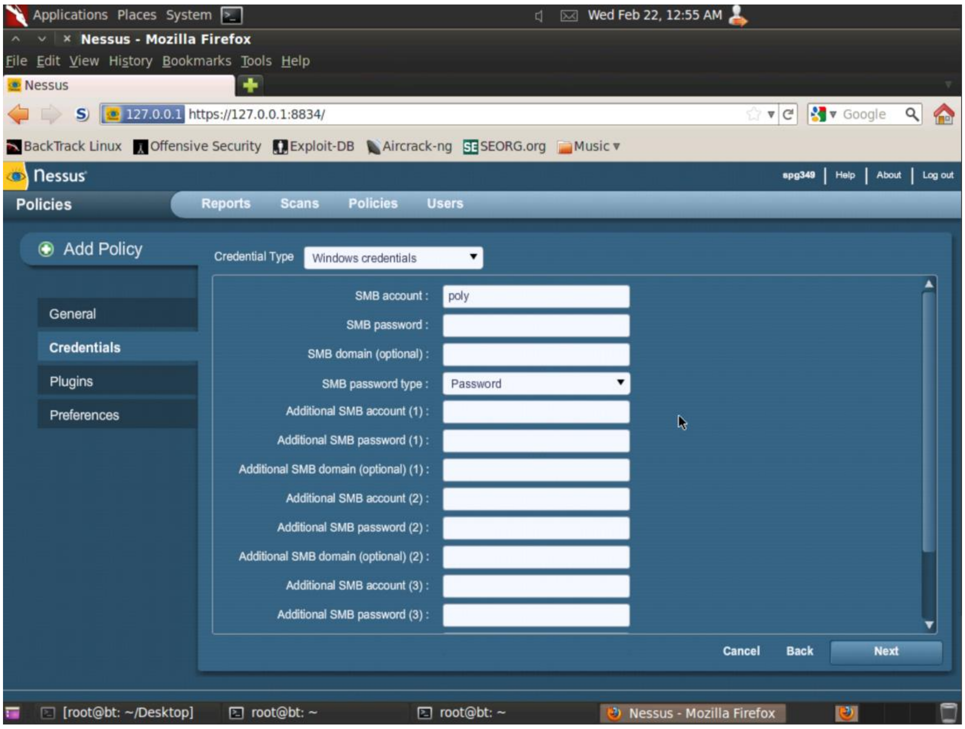
Scan
Save Knowledge Base □
Safe Checks □
Silent Dependencies □
Log Scan Details to Server □
Stop Host Scan on Disconnect □
Avoid Sequential Scans □
Consider Unscanned Ports as Closed □
Designate Hosts by their DNS Name □

Network Congestion
Reduce Parallel Connections on Congestion □
Use Kernel Congestion Detection (Linux Only) □

Port Scanners
TCP Scan ☑ SNMP Scan ☑ Ping Host ☑
UDP Scan □ Netstat SSH Scan ☑
SYN Scan ☑ Netstat WMI Scan ☑

Port Scan Options
Port Scan Range: 1-65535

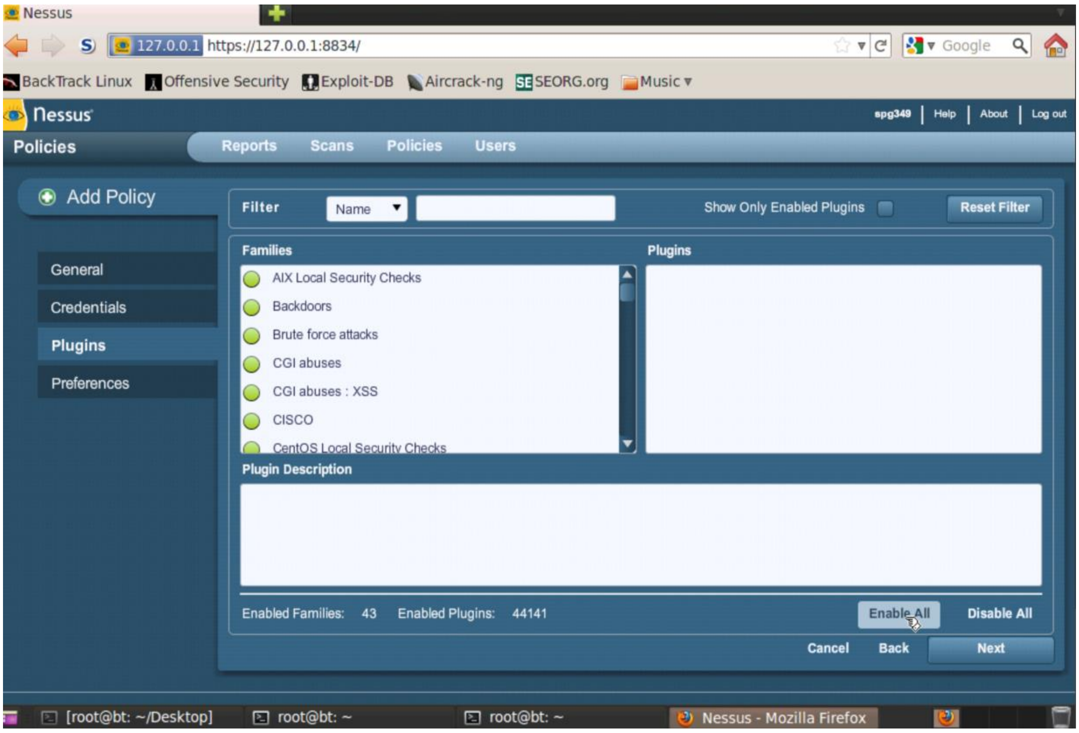
Performance
Max Checks Per Host: 5
Max Hosts Per Scan: 100
Network Receive Timeout (seconds): 5
Max Simultaneous TCP Sessions Per Host: unlimited
Max Simultaneous TCP Sessions Per Scan: unlimited

- On the Credentials section
    - Set the Windows credentials with “poly” and password “” based on the Vital Wiki Lab0 Guide
    - Based on the nmap scan results found that no Web,SSH or Telnet Protocols [or Ports were open] are enabled hence did not set any credentials for other protocols (Others – default)
    - 

Add Policy — Credentials

Credential Type: Windows credentials
SMB account : poly
SMB password :
SMB domain (optional) :
SMB password type : Password
Additional SMB account (1) :
Additional SMB password (1) :
Additional SMB domain (optional) (1) :
Additional SMB account (2) :
Additional SMB password (2) :
Additional SMB domain (optional) (2) :
Additional SMB account (3) :
Additional SMB password (3) :

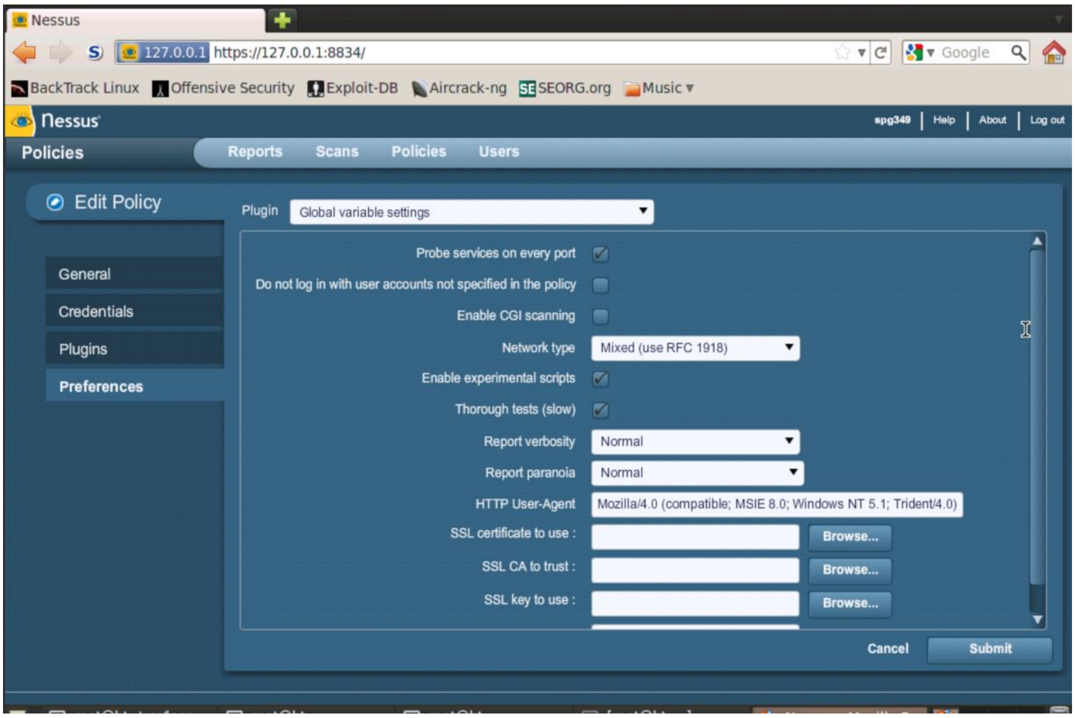
- Plugins Section
  - Enabled All the Plugins for all kinds of vulnerability CVE



Families:
- ● AIX Local Security Checks
- ● Backdoors
- ● Brute force attacks
- ● CGI abuses
- ● CGI abuses : XSS
- ● CISCO
- ● CentOS Local Security Checks

Enabled Families: 43 Enabled Plugins: 44141

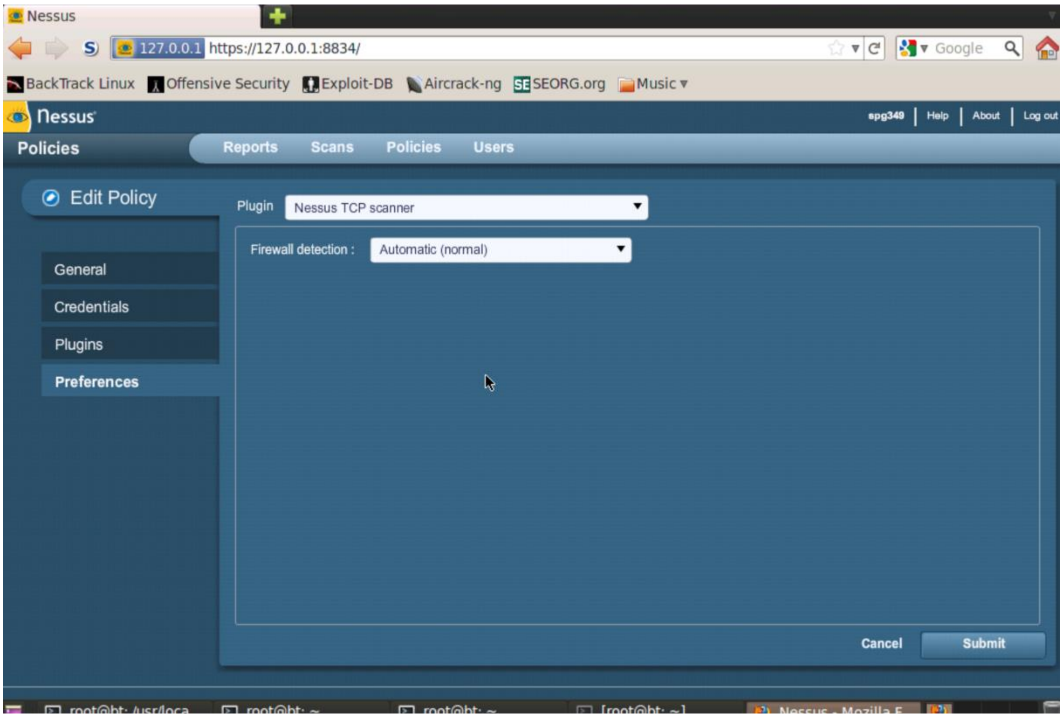
- Preferences Section
  - Global Variable Setting
    - Enabling Experimental Scripts and Thorough Test – to make sure any chance of vulnerability occurrence in the target. Web services ignored as the no web services are enabled according to the Nessus scan.



Plugin: Global variable settings

Probe services on every port ☑
Do not log in with user accounts not specified in the policy □
Enable CGI scanning □
Network type: Mixed (use RFC 1918)
Enable experimental scripts ☑
Thorough tests (slow) ☑
Report verbosity: Normal
Report paranoia: Normal
HTTP User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
SSL certificate to use :
SSL CA to trust :
SSL key to use :

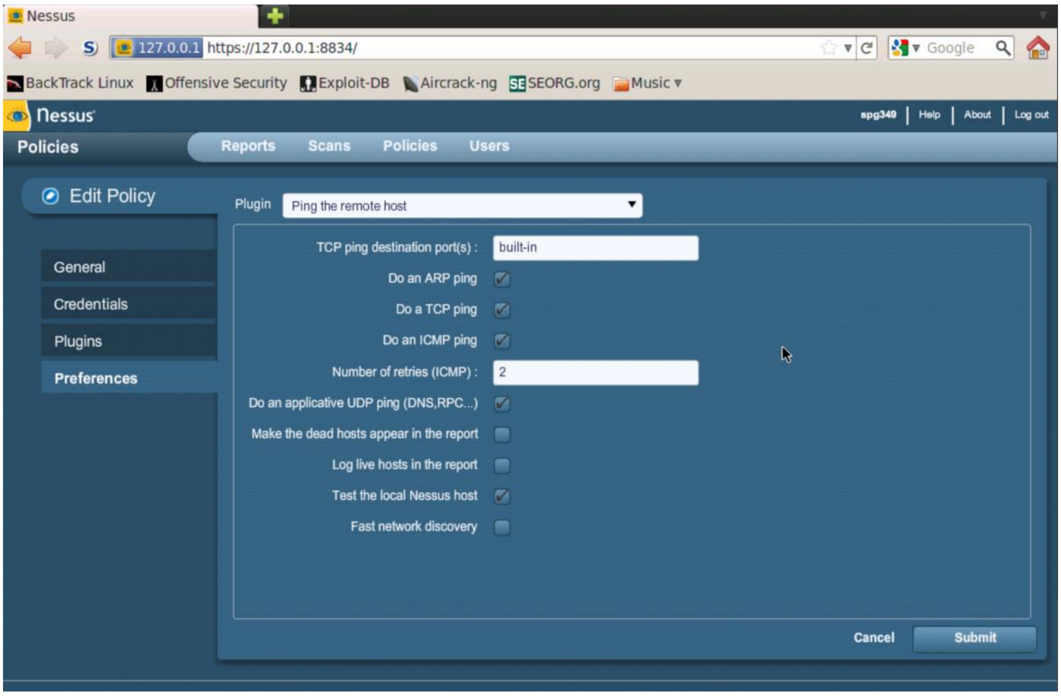
- Nessus TCP/SYN Scanner – to Automatic Firewall Detection



Plugin: Nessus TCP scanner

Firewall detection : Automatic (normal)

- Enable UDP Ping to perform any UDP checks



Plugin: Ping the remote host

TCP ping destination port(s) : built-in

Do an ARP ping ☑

Do a TCP ping ☑

Do an ICMP ping ☑

Number of retries (ICMP) : 2

Do an applicative UDP ping (DNS,RPC...) ☑

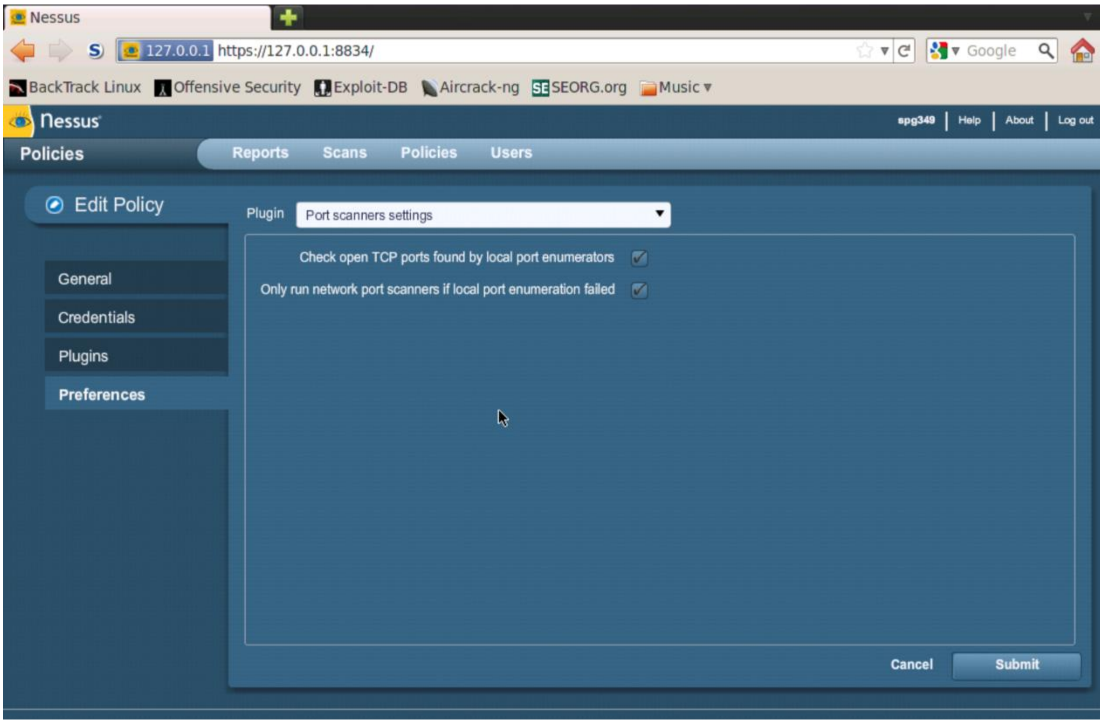
Make the dead hosts appear in the report □

Log live hosts in the report □

Test the local Nessus host ☑

Fast network discovery □

- Using Port enumerators for faster port scanning and port scanners when port enumeration fails
  Reference: https://community.tenable.com/thread/1337

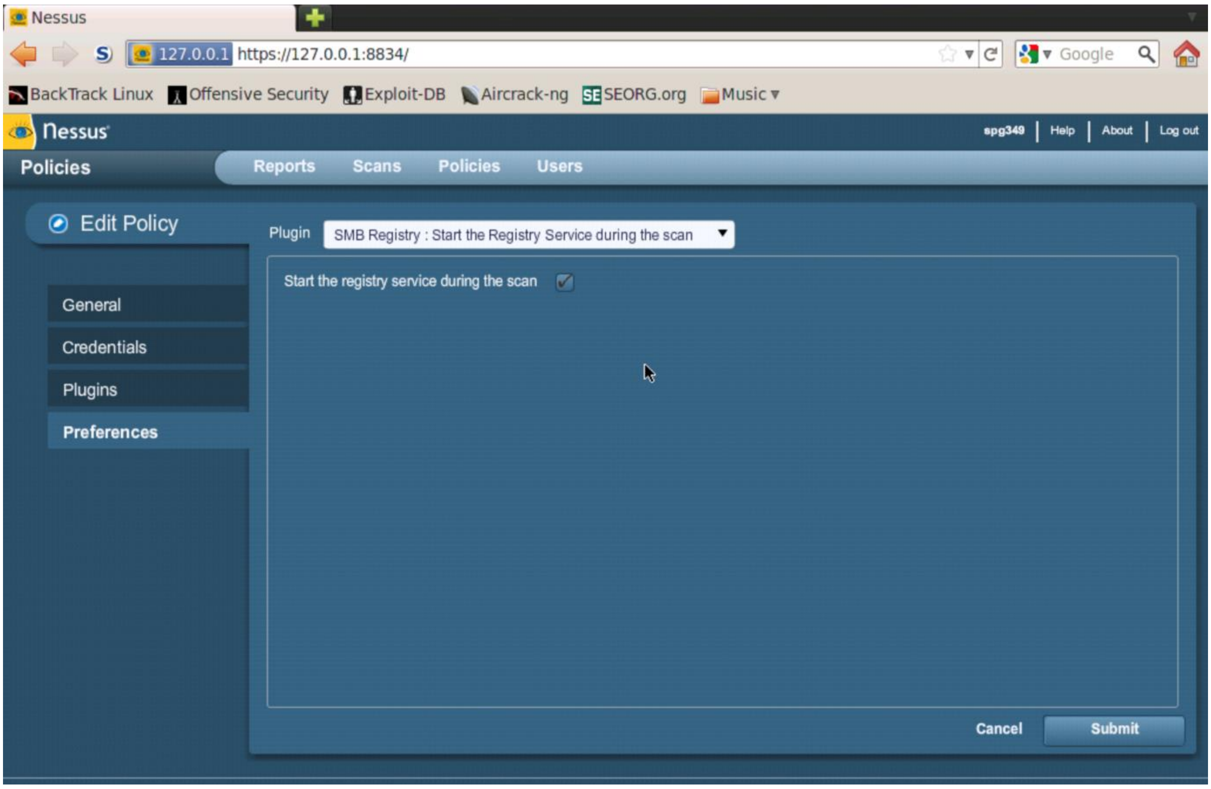


Plugin: Port scanners settings

Check open TCP ports found by local port enumerators ☑

Only run network port scanners if local port enumeration failed ☑

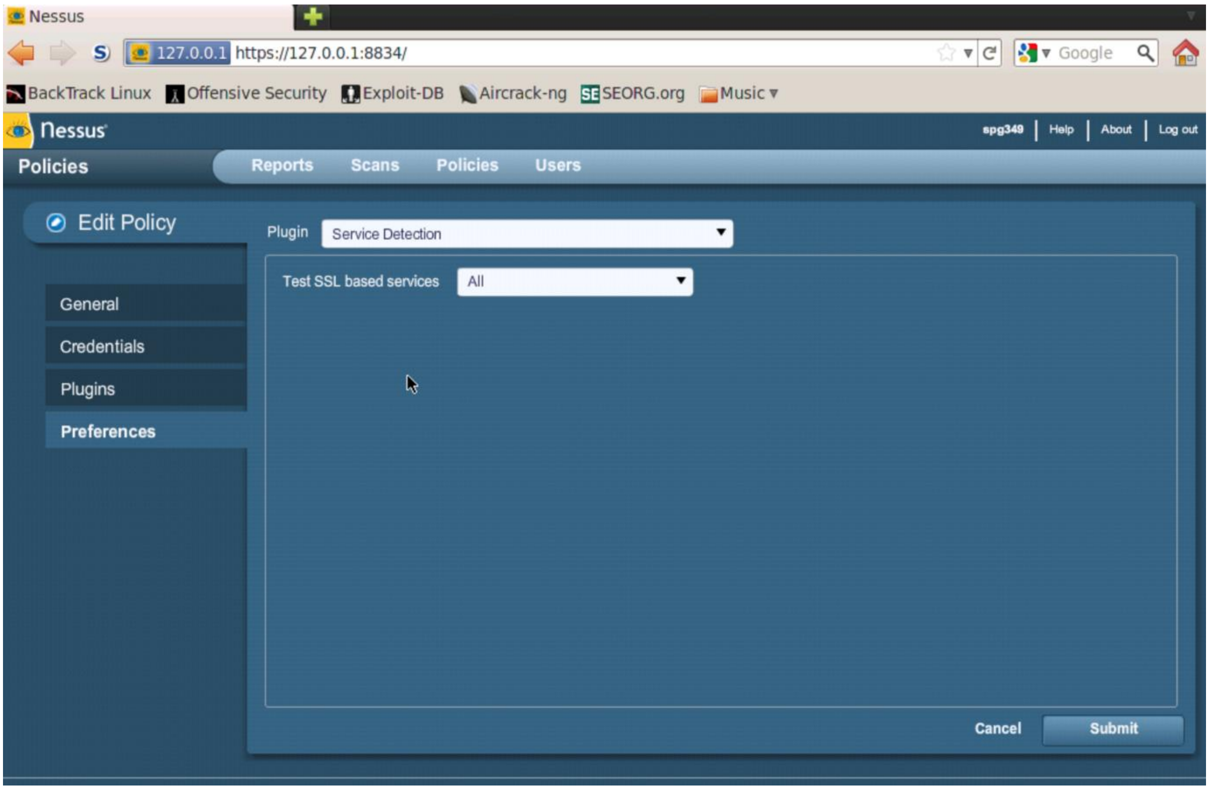
- SMB Registry Start: Knowing that the SMB registry port is open and the service existence in the windows machine from nmap (139,445), enabled this option to enable if it is down.



Plugin: SMB Registry : Start the Registry Service during the scan

Start the registry service during the scan ☑

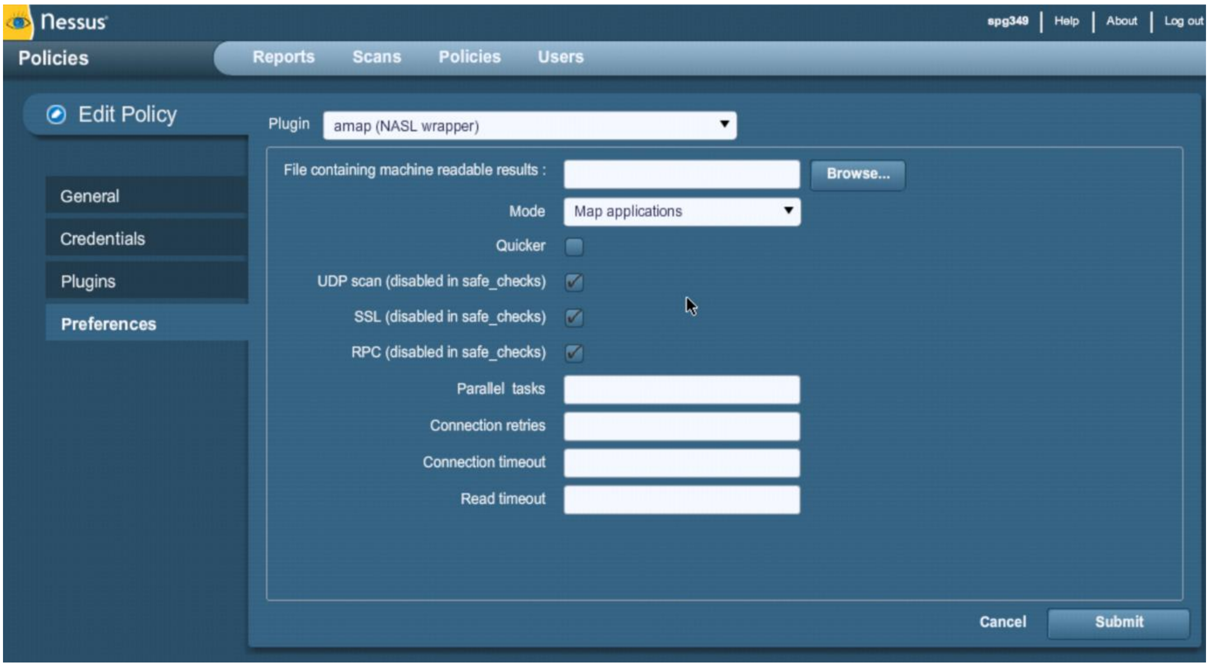
- Service Detection – Set to ALL instead of know SSL ports to ensure If anything at all was missed during nmap scan



Plugin: Service Detection

Test SSL based services: All

- AMAP Scanner (Identify Applications irrespective of ports) – To scan UDP Ports
  - Enabled UDP Scan and others are default



Plugin: amap (NASL wrapper)

File containing machine readable results :

Mode: Map applications

Quicker ☐

UDP scan (disabled in safe_checks) ☑

SSL (disabled in safe_checks) ☑

RPC (disabled in safe_checks) ☑

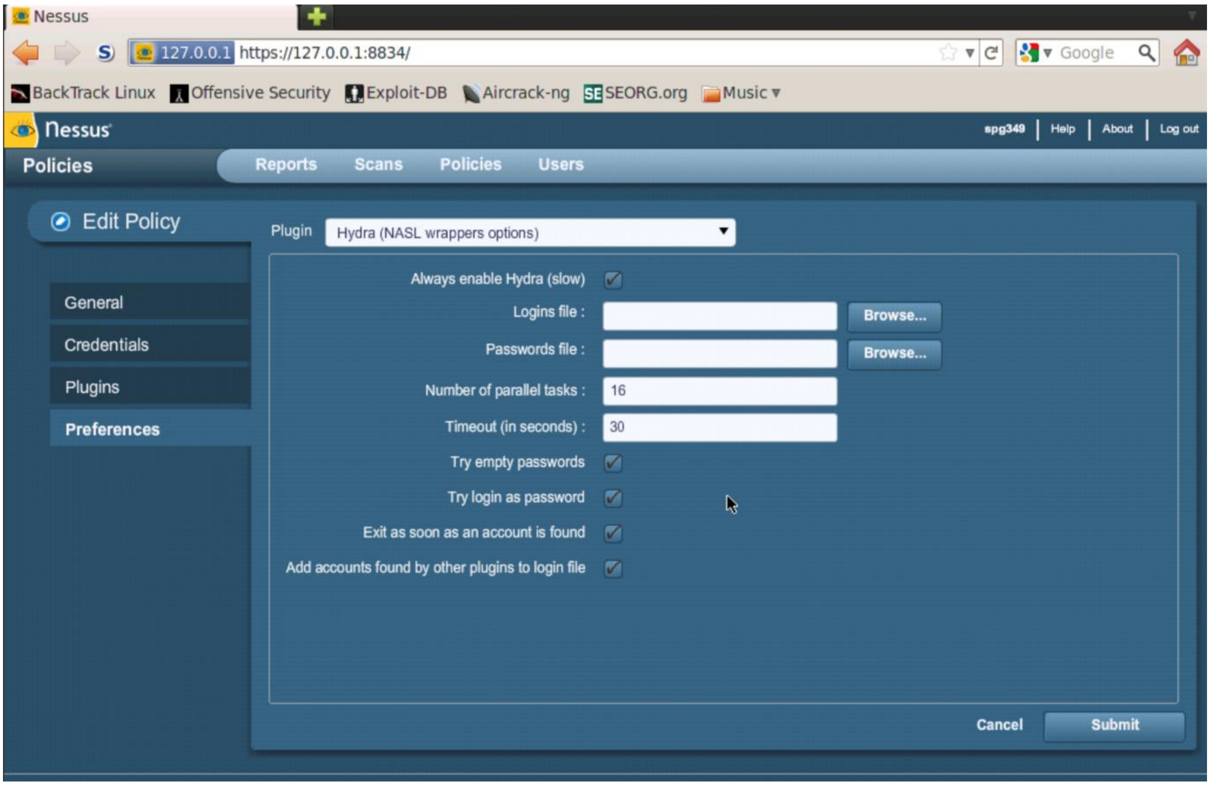
Parallel tasks

Connection retries

Connection timeout

Read timeout

- HYDRA Scanner (Login Cracker)–
  - Enabled Hydra Scanner and Hydra SMB scan option



Plugin: Hydra (NASL wrappers options)

Always enable Hydra (slow) ☑
Logins file :
Passwords file :
Number of parallel tasks : 16
Timeout (in seconds) : 30
Try empty passwords ☑
Try login as password ☑
Exit as soon as an account is found ☑
Add accounts found by other plugins to login file ☑

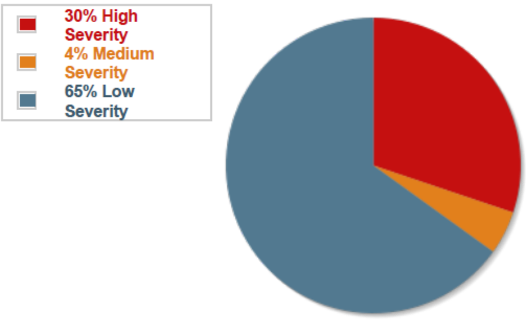
- All the other options (SNMP, Web) are set to default as no TCP/UDP Port were detected in nmap scan

# Scan Results :

## ---- *Scan Summary*

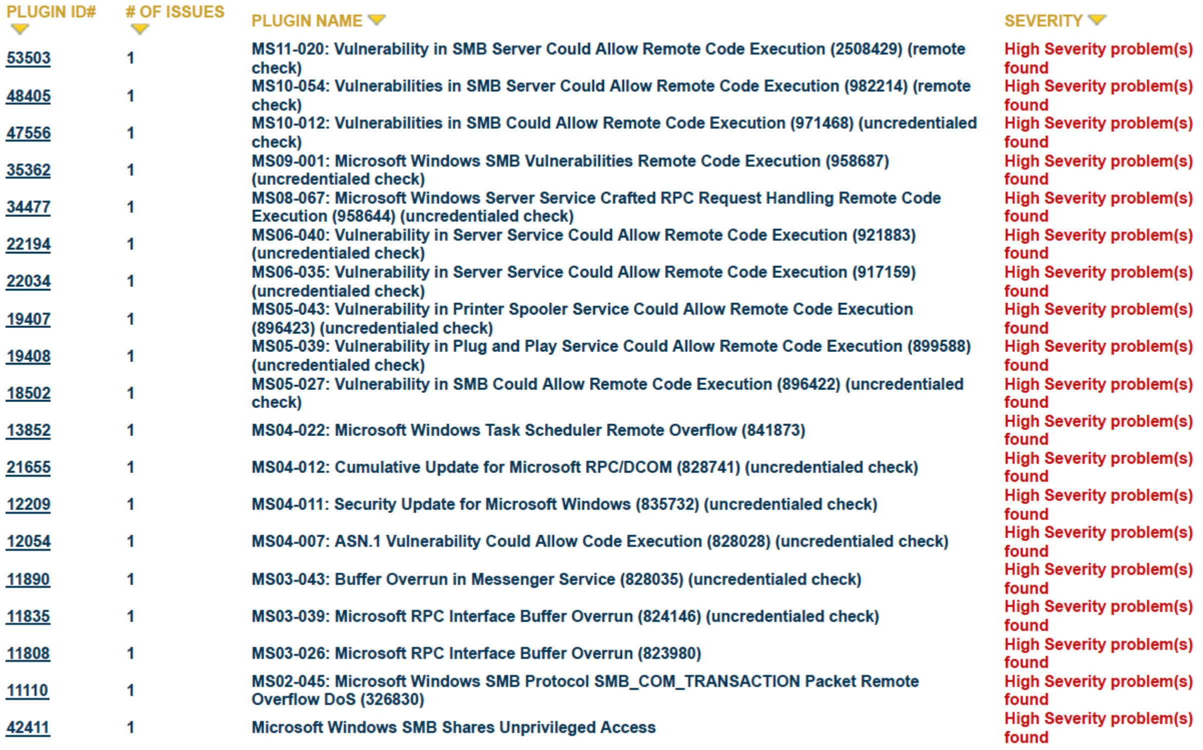
### Executive Summary:

TOP 10 HOSTS with ISSUES



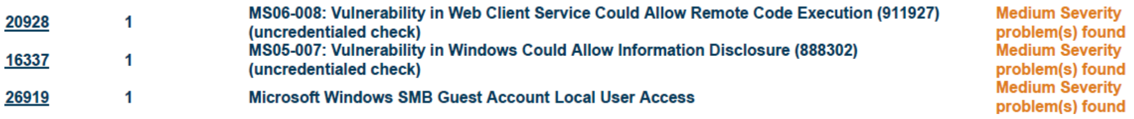
10.10.111.110 High Severity problem(s) found

# *High Severity Vulnerability:*



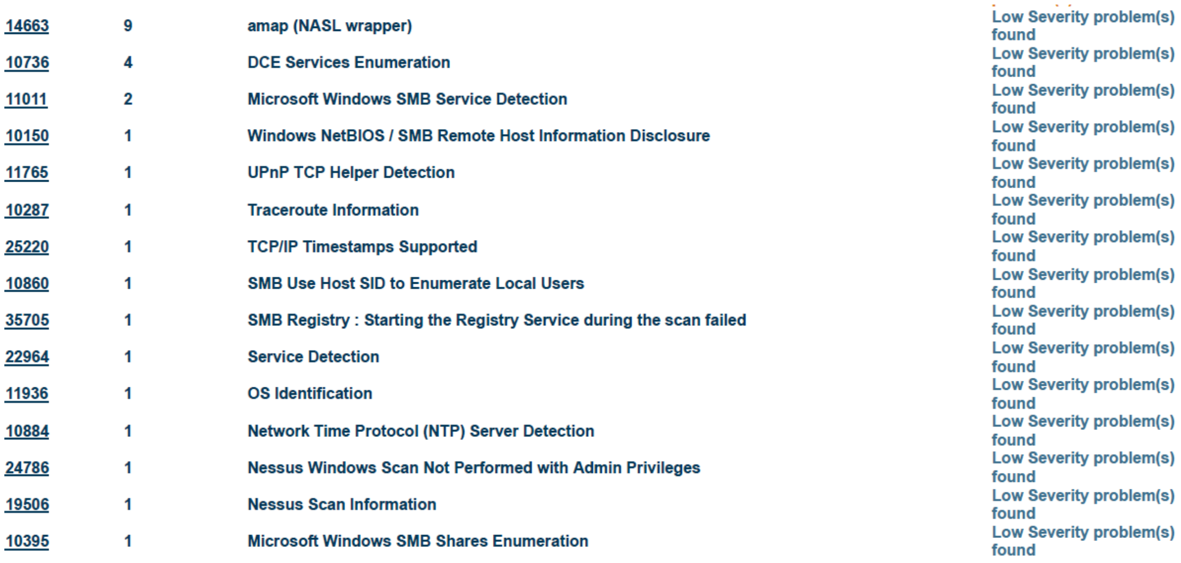
| PLUGIN ID# ▼ | # OF ISSUES ▼ | PLUGIN NAME ▼ | SEVERITY ▼ |
|---|---|---|---|
| 53503 | 1 | MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check) | High Severity problem(s) found |
| 48405 | 1 | MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check) | High Severity problem(s) found |
| 47556 | 1 | MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check) | High Severity problem(s) found |
| 35362 | 1 | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) | High Severity problem(s) found |
| 34477 | 1 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check) | High Severity problem(s) found |
| 22194 | 1 | MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check) | High Severity problem(s) found |
| 22034 | 1 | MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check) | High Severity problem(s) found |
| 19407 | 1 | MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check) | High Severity problem(s) found |
| 19408 | 1 | MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check) | High Severity problem(s) found |
| 18502 | 1 | MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) | High Severity problem(s) found |
| 13852 | 1 | MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) | High Severity problem(s) found |
| 21655 | 1 | MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check) | High Severity problem(s) found |
| 12209 | 1 | MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check) | High Severity problem(s) found |
| 12054 | 1 | MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) | High Severity problem(s) found |
| 11890 | 1 | MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check) | High Severity problem(s) found |
| 11835 | 1 | MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check) | High Severity problem(s) found |
| 11808 | 1 | MS03-026: Microsoft RPC Interface Buffer Overrun (823980) | High Severity problem(s) found |
| 11110 | 1 | MS02-045: Microsoft Windows SMB Protocol SMB_COM_TRANSACTION Packet Remote Overflow DoS (326830) | High Severity problem(s) found |
| 42411 | 1 | Microsoft Windows SMB Shares Unprivileged Access | High Severity problem(s) found |

# *Medium Severity:*

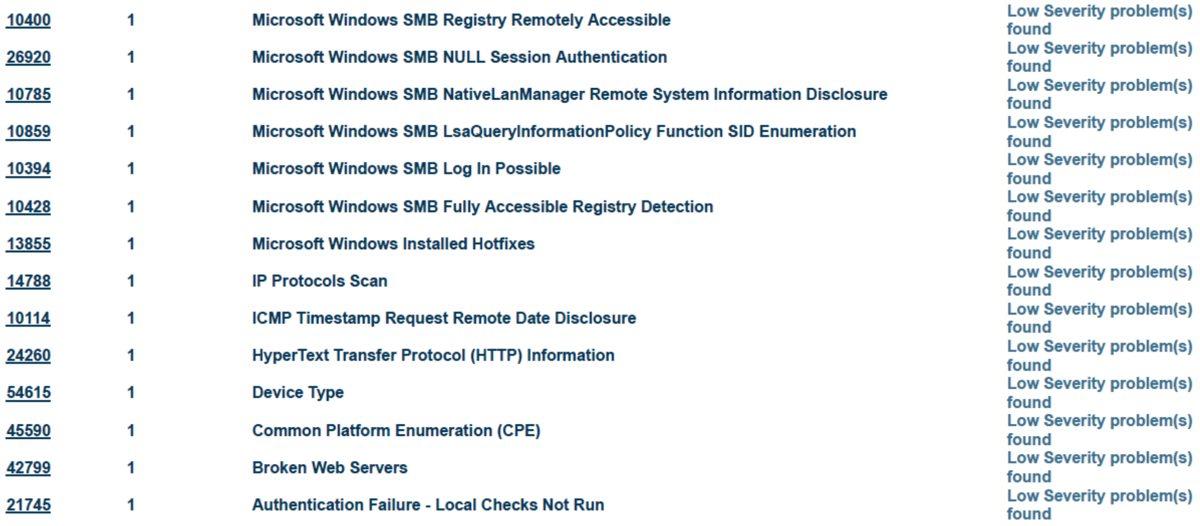


| | | | |
|---|---|---|---|
| 20928 | 1 | MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution (911927) (uncredentialed check) | Medium Severity problem(s) found |
| 16337 | 1 | MS05-007: Vulnerability in Windows Could Allow Information Disclosure (888302) (uncredentialed check) | Medium Severity problem(s) found |
| 26919 | 1 | Microsoft Windows SMB Guest Account Local User Access | Medium Severity problem(s) found |

# Low Severity:

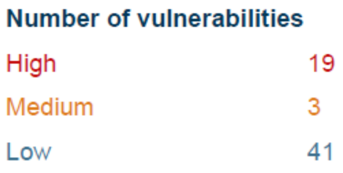


| | | | |
|---|---|---|---|
| 14663 | 9 | amap (NASL wrapper) | Low Severity problem(s) found |
| 10736 | 4 | DCE Services Enumeration | Low Severity problem(s) found |
| 11011 | 2 | Microsoft Windows SMB Service Detection | Low Severity problem(s) found |
| 10150 | 1 | Windows NetBIOS / SMB Remote Host Information Disclosure | Low Severity problem(s) found |
| 11765 | 1 | UPnP TCP Helper Detection | Low Severity problem(s) found |
| 10287 | 1 | Traceroute Information | Low Severity problem(s) found |
| 25220 | 1 | TCP/IP Timestamps Supported | Low Severity problem(s) found |
| 10860 | 1 | SMB Use Host SID to Enumerate Local Users | Low Severity problem(s) found |
| 35705 | 1 | SMB Registry : Starting the Registry Service during the scan failed | Low Severity problem(s) found |
| 22964 | 1 | Service Detection | Low Severity problem(s) found |
| 11936 | 1 | OS Identification | Low Severity problem(s) found |
| 10884 | 1 | Network Time Protocol (NTP) Server Detection | Low Severity problem(s) found |
| 24786 | 1 | Nessus Windows Scan Not Performed with Admin Privileges | Low Severity problem(s) found |
| 19506 | 1 | Nessus Scan Information | Low Severity problem(s) found |
| 10395 | 1 | Microsoft Windows SMB Shares Enumeration | Low Severity problem(s) found |



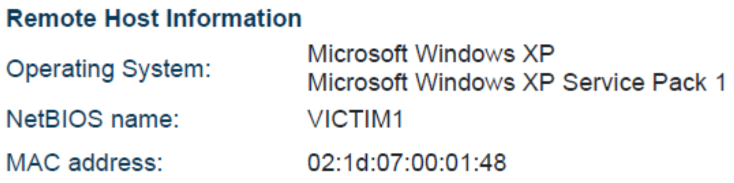
| | | | |
|---|---|---|---|
| 10400 | 1 | Microsoft Windows SMB Registry Remotely Accessible | Low Severity problem(s) found |
| 26920 | 1 | Microsoft Windows SMB NULL Session Authentication | Low Severity problem(s) found |
| 10785 | 1 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure | Low Severity problem(s) found |
| 10859 | 1 | Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration | Low Severity problem(s) found |
| 10394 | 1 | Microsoft Windows SMB Log In Possible | Low Severity problem(s) found |
| 10428 | 1 | Microsoft Windows SMB Fully Accessible Registry Detection | Low Severity problem(s) found |
| 13855 | 1 | Microsoft Windows Installed Hotfixes | Low Severity problem(s) found |
| 14788 | 1 | IP Protocols Scan | Low Severity problem(s) found |
| 10114 | 1 | ICMP Timestamp Request Remote Date Disclosure | Low Severity problem(s) found |
| 24260 | 1 | HyperText Transfer Protocol (HTTP) Information | Low Severity problem(s) found |
| 54615 | 1 | Device Type | Low Severity problem(s) found |
| 45590 | 1 | Common Platform Enumeration (CPE) | Low Severity problem(s) found |
| 42799 | 1 | Broken Web Servers | Low Severity problem(s) found |
| 21745 | 1 | Authentication Failure - Local Checks Not Run | Low Severity problem(s) found |

*Machine Details and Summary:*



**Number of vulnerabilities**

| | |
|---|---|
| High | 19 |
| Medium | 3 |
| Low | 41 |



**Remote Host Information**

| | |
|---|---|
| Operating System: | Microsoft Windows XP<br>Microsoft Windows XP Service Pack 1 |
| NetBIOS name: | VICTIM1 |
| MAC address: | 02:1d:07:00:01:48 |

# 3. Summary:

Based on the Scan reports, we have found the TCP/UDP ports, services running and vulnerabilities present in the hosts. With these Information, we could exploit the protocols and vulnerabilities by,

* As we get to know that DHCP and DNS are open in most of the linux Operating Systems, we could perform attacks like Rogue DHCP or DHCP Starvation or DNS Poisoning attacks.

* The Windows machine obviously vulnerable from the findings can be exploited with SMB Server attacks, Buffer Overrun and Remote Code Execution attacks.

* The Last linux machine 110.111 has a MySQL server open unauthorized for access which can be exploited

* Based on the OS, Service and Version information obtained we can easily check through vulnerability database in the internet to find a possible exploit without the fix in the current version and attack it.